**IT Applications, Unit 4**

Security and ethical considerations, Ch 8, p 285

**Security Equipment**

**SECURITY HARDWARE**

1. **What is meant by data integrity?**

Data integrity is the assurance that data is accurate and reliable, and is available in a timely manner.

**BIOMETRICS**

* 1. **Describe biometric security.**

Biometric security is the use of Physical human characteristics , including finger prints or facial features, behavioural characteristics such as voice patterns or handwriting to authenticate a user before granting access to data.

* 1. **Why does it appeal to security managers?**

This system appeals to security managers as it is nearly impossible to copy steal an individual’s biometric characteristics.

* 1. **List the common biometric devices.**
* Voice recognition
* Fingerprint recognition
* Hand geometry
* Facial recognition
* Iris recognition
  1. **What are the concerns of biometric technology?**

The main concerns of users are the perceived intrusiveness of the technology. For example many people currently consider iris scanning less acceptable than finger print scanning or voice recognition as it focuses on the eyes. Another limitation relates to the cost.

**SWIPE CARDS**

1. **Describe the nature of a swipe card.**

Swipe cards are usually business sized plastic card with a magnetic strip on one side with the user details on the other; for example credit cards and ATM cards. The magnetic strip contains information about the owner of the card, including a personal identification number, or PIN.

1. **What is a limitation of the swipe card?**

One limitation is that it can be easily damaged by magnetic fields. Also if stolen they offer little protection from a thief with a swipe-card reader that can capture the data on it.

**SMART CARDS**

1. **What is a Smart Card?**

Similar to the swipe card, except the smart card has a microchip embedded in it to store and manipulate data. Examples include; prepaid phone cards, photocopy card and Myki public transport cards in Melbourne.

**SECURITY TOKENS**

1. **What is a Security token?**

A security token is a small device that displays a constantly changing authentication code. If the user wishes to use

**MOBILE PHONE SECURE CODE**

1. **How does this level of authentication work?**

This system works by sending a security code to the account holder’s mobile phone to authenticate a transaction before it actually occurs. The account holder then needs to log in and enter the code before the transaction can be processed.

**POWER PROTECTION**

**Outline the characteristics of the following:**

1. **Surge protector**

This basic device protects electrical equipment against overvoltage caused by a power surge. It smoothes the current coming from the mains supply and will block sudden surges.

1. **Uninterruptible power supply, (UPS)**

A UPS is a high-quality surge protector and battery built into the one device. As well as guarding a spike, it will protect data if there is an undercurrent or complete power failure.

**STRATEGIES FOR AVOIDING SYSTEM FAILURE, P 288**

1. **What is meant by redundancy?**

Redundancy means no single part of the system is critical to its overall operation.

1. **What is meant be a fault-tolerant server?**

If one part fails, other parts, hard drives or mirrored machines, can take over and keep the system running.

**REDUNDANCY THROUGH MULTIPLE HARD DRIVES OR FAULT-TOLERANT EQUIPMENT**

* 1. **Describe how this redundancy works.**

A common solution is to continuously copy the data onto a second, ‘mirrored’ hard drive. If the main drive fails, then a duplicate set of data is available on the mirrored drive.

* 1. **What is meant by RAID technology**

Redundant Array of Inexpensive Disks or RAID technology is commonly used on a computer network and works by spreading fragments of data over several hard drives, so that if one hard drive fails, the others can piece together the missing data and rebuild the file using error-checking codes.

**REDUNDANCY THROUGH MIRRORED SERVERS OR MACHINES**

1. **Why is the RAID solution preferable to this solution?**

A mirrored computer/server is a much more expensive option. Redundant array of inexpensive disks (RAID) is a protection system fragments of data are spread over several hard drives. This is so that if one disk fails the others can piece together the missing data and rebuild the file using error-checking codes.

**BACKUP MEDIA**

1. **There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?**

* The cost of the drive or writer
* The cost of media per GB
* Speed and compatibility.

1. **Three categories of backup media:**

* Magnetic media
* Optical drives
* Solid-state drives

**LIST THE CHARACTERISTICS OF THE FOLLOWING BACKUP MEDIA:**

**Magnetic media**

1. **Hard Disk Drive**

Affordable option to back up files

1. **Magnetic Tapes**

Relatively cheap, but are slow to save and restore files, as the tape must be read and accessed sequentially.

**OPTICAL MEDIA**

1. **Compact Disc**

Compact disks are removable storage media that can hold up to 700 MB of data and come as either CD-Read, which can only be used once, or CD-RW, which allows you to use the disk multiple times.

1. **DVD**

DVDs can store up to 17 GB of data, can be used once (DVD-R) or many times (DVD-RW).

1. **Blu-ray**

Optical disk format with a capacity of 50 GB, allows HD videos to be stored on it.

**SOLID-STATE DRIVES**

1. **USB storage devices**

Storage devices that are usually small. Convenient as there are no moving parts, the memory is solid state, and therefore there is less chance of a breakdown. USB flash drive can hold up to 256 GB.

**ONLINE BACKUPS**

1. **Why do organisations use this form of backup?**

So that storage and backup have been consolidated (combined) together. This ensures that they work as efficiently and effectively as possible.

1. **Describe an enterprise storage system.**

A system that involves the interconnection via a storage area network (SAN), of RAID disks, tapes, CD/DVD-ROM servers, Internet backup and other network storage devices.

**SURVEILLANCE TECHNOLOGY, P 292**

**Describe the nature of the following items of surveillance equipment used in offices:**

1. **Packet sniffers**

Diagnostic tools that monitor the contents of packets sent across networks. They can be set to filter packets to an admins computer for further analysis.

1. **Desktop monitoring programs**

Software that monitors every action performed on a computer. Hackers often use a Trojan Horse virus to install this type of software.

1. **Log files**

These are the computer itself recording events. Web servers will record all the URL’ s accessed while mail servers will record all email sent.

1. **Closed-circuit television, (CCTV)**

A series of video cameras linked to an internal TV system. Usually watched by security guards.

1. **Telephones**

Employers will often tap certain phones. In most cases, they wish to ensure that all phone conversations are kept to only company business. Call centres might do so ensure that a high standard of customer service s delivered.

1. **Audit trails**

The combination of surveillance equipment mentioned above. This can b made by linking various logs or recordings of system activity.

**PHYSICAL SECURITY DEVICES**

1. **List the options for physically securing your data**

* Lockable disk box
* Safe
* Specialised temperature monitoring rooms
* Security cables